

# $\mathbf{F}_p$ -representations over $p$ -fields

Chandan Singh Dalawat  
 Harish-Chandra Research Institute  
 Chhatnag Road, Jhansi, Allahabad 211019, India  
 dalawat@gmail.com

**Abstract.** Let  $p$  be a prime,  $k$  a finite extension of  $\mathbf{F}_p$  of cardinal  $q$ ,  $l$  a finite extension of  $k$  of group  $\Sigma = \text{Gal}(l|k)$ , and  $T$  a subgroup of  $l^\times$ . Using the method of “little groups”, we classify irreducible  $\mathbf{F}_p$ -representations of the group  $G = T \times_q \Sigma$ , the twisted product of  $\Sigma$  with the  $\Sigma$ -module  $T$ . We then use these results to classify irreducible continuous  $\mathbf{F}_p$ -representations of the profinite group  $\text{Gal}(\tilde{K}|K)$  of  $K$ -automorphisms of the maximal galoisian extension  $\tilde{K}$  of a  $p$ -field  $K$  with residue field  $k$ .

## 1. Introduction

(1) Let  $p$  be a prime and let  $K$  be a  $p$ -field, namely a local field with finite residue field of characteristic  $p$ . Let  $\tilde{K}$  be a maximal galoisian extension of  $K$ . Let  $V$  be the maximal tamely ramified extension of  $K$  in  $\tilde{K}$ . All representations of the profinite groups  $\text{Gal}(\tilde{K}|K)$  and  $\text{Gal}(V|K)$  appearing below are assumed to be *continuous*. The ramification group  $\text{Gal}(\tilde{K}|V)$ , which is a pro- $p$ -group, acts trivially on any irreducible  $\mathbf{F}_p$ -representation of  $\text{Gal}(\tilde{K}|K)$ . So classifying irreducible  $\mathbf{F}_p$ -representations of  $\text{Gal}(\tilde{K}|K)$  comes down to classifying irreducible  $\mathbf{F}_p$ -representations of  $\text{Gal}(V|K)$ , which comes down to classifying irreducible  $\mathbf{F}_p$ -representations of  $\text{Gal}(L|K)$  for every finite tamely ramified galoisian extensions  $L$  of  $K$ .

(2) For such  $L$  with group of  $K$ -automorphisms  $G = \text{Gal}(L|K)$  and inertia subgroup  $G_0$ , the projection  $G \rightarrow G/G_0$  need not have a section, but  $L$  has finite unramified extensions  $L'$  for which the corresponding projections  $G' \rightarrow G'/G'_0$  (where  $G'$  is  $\text{Gal}(L'|K)$  and  $G'_0$  is its inertia subgroup) do have sections ; the smallest such  $L'$  is the one whose degree over  $L$  is equal to the order in  $H^2(G/G_0, G_0)$  of the class of the extension  $G$  of  $G/G_0$  by the  $(G/G_0)$ -module  $G_0$  ; see for example [3, Lemma 2.3.4]. So it is enough to understand irreducible  $\mathbf{F}_p$ -representations of  $G$  in this

---

*MSC2010* : Primary 11F80, 11S99, 20C20

*Keywords* : Local fields, Galois representations, Little groups

*split* case ; with a heavy heart, we choose a section of  $G \rightarrow G/G_0$  in what follows.

(3) Our treatment, which is completely canonical and somewhat simpler than in the literature, is better adapted to this arithmetic application because the inertia group  $G_0$  does not come with a generator, only a canonical character  $\theta : G_0 \rightarrow l^\times$ , where  $l$  is the residue field of  $L$ . It is based upon §7 of [9, p. 205] and the method of “little groups” of Wigner and Mackey as exposed in §8.2 of [11, p. 62] ; I thank my friend UK Anandavardhanan for pointing out the latter reference. The material is also worked out in §4.1 of [7, p. 329].

(4) Let  $k$  be the residue field of  $K$  ; the quotient  $\Sigma = G/G_0$  can be identified with  $\text{Gal}(l|k)$ , which has the canonical generator  $\sigma : x \mapsto x^q$  ( $x \in l$ ), where  $q = \text{Card } k$ . The conjugation action of  $\Sigma$  on  $G_0$  is given by  $\sigma.t = t^q$  for every  $t \in G_0$  ; the character  $\theta$  is  $\Sigma$ -equivariant. To determine the  $\mathbf{F}_p$ -representations of  $G$ , we may forget the fields  $K$  and  $L$ , and retain only  $p$ ,  $k$ ,  $l$ , and  $e = \text{Card } G_0$ . This is done in §2. In §3, we return to these local fields and make an observation which will be useful elsewhere [5].

## 2. Irreducible $\mathbf{F}_p$ -representations of little groups

(5) *Notation.* Let us restart and rename. Fix a prime number  $p$ , fix a finite extension  $k$  of  $\mathbf{F}_p$ , put  $q = \text{Card } k$ , fix a finite extension  $l$  of  $k$ , put  $f = [l : k]$ , and denote by  $\sigma : x \mapsto x^q$  ( $x \in l$ ) the canonical generator of  $\Sigma = \text{Gal}(l|k)$ . Let  $T \subset l^\times$  be a subgroup, let  $e$  be the order of  $T$  (so that  $q^f \equiv 1 \pmod{e}$ ), and let  $\theta : T \rightarrow l^\times$  be the inclusion (viewed as a character). Finally, let  $G = T \times_q \Sigma$  be the twisted product of  $\Sigma$  with the  $\Sigma$ -module  $T$  (for the galoisian action  $\sigma.t = \sigma t \sigma^{-1} = t^q$  ( $t \in T$ )). Notice that the action is trivial, or equivalently  $G$  is commutative, if and only if  $q \equiv 1 \pmod{e}$ .

(6) *The problem.* Classify irreducible  $\mathbf{F}_p$ -representations of  $G$ .

(7) *Notation.* For every character  $\chi : T \rightarrow l^\times$ , we denote by  $d_\chi$  the order of  $\chi$  and by  $r_\chi$  (resp.  $s_\chi$ ) the order of the image  $\bar{p}$  (resp.  $\bar{q}$ ) in  $(\mathbf{Z}/d_\chi \mathbf{Z})^\times$ . Put  $T_\chi = T / \text{Ker}(\chi)$  and let  $\Sigma_\chi$  be the kernel of the action of  $\Sigma$  on  $T_\chi$  ; the group  $\Sigma_\chi$  is generated by  $\sigma^{s_\chi}$ , and  $s_\chi$  is also the size of the  $\Sigma$ -orbit  $\bar{\chi}$  of  $\chi$ . We have the subgroup  $G_\chi = T \times_q \Sigma_\chi$  of  $G$  and the quotient  $\bar{G}_\chi = T_\chi \times \Sigma_\chi$  of  $G_\chi$  which is commutative by construction. The numbers  $d_\chi$ ,  $r_\chi$ ,  $s_\chi$ , the groups  $\Sigma_\chi$ ,  $G_\chi$ ,  $\bar{G}_\chi$ , and some characters of these groups to be defined presently, depend only on the  $\Sigma$ -orbit  $\bar{\chi}$  of  $\chi$  ; we keep the notation light by writing  $\chi$  in the subscript instead of  $\bar{\chi}$ . Let  $\chi$  also stand for the faithful character  $T_\chi \rightarrow l^\times$  coming from  $\chi$ .

(8) We begin by determining the *irreducible  $\tilde{l}$ -representations* of  $G$ , where  $\tilde{l} = l(\sqrt[p]{f})$ ,  $f' = fp^{-v_p(f)}$ , and  $v_p(f)$  is the exponent of  $p$  in the prime decomposition of  $f$ ; they will turn out to be absolutely irreducible. These representations will be parametrised by pairs  $(\bar{\chi}, \lambda)$ , where  $\bar{\chi} \subset \text{Hom}(T, l^\times)$  is the  $\Sigma$ -orbit of a character  $\chi : T \rightarrow l^\times$  (for the action  $\sigma : \chi \mapsto \chi^q$ ) and  $\lambda \in \tilde{l}^\times$  is an element of order dividing  $fs_\chi^{-1}$ . This is achieved in several steps.

(9) *The  $\tilde{l}$ -representation  $\rho_{\bar{\chi}, \lambda}$  of  $G$  associated to a pair  $(\bar{\chi}, \lambda)$ .* Choose  $\chi \in \bar{\chi}$ , and let  $\psi_{\chi, \lambda} : \Sigma_\chi \rightarrow \tilde{l}^\times$  be the unique character such that  $\psi_{\chi, \lambda}(\sigma^{s_\chi}) = \lambda$ . View the character  $\chi \otimes \psi_{\chi, \lambda}$  of  $\bar{G}_\chi = T_\chi \times \Sigma_\chi$  as a character of  $G_\chi = T \times_q \Sigma_\chi$ , and take the induced representation  $\rho_{\bar{\chi}, \lambda} = \text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$ .

(10) To see that  $\rho = \rho_{\bar{\chi}, \lambda}$  depends only on the pair  $(\bar{\chi}, \lambda)$ , and for later use, let us make all this explicit. The quotient  $G/G_\chi$  is generated by the image of  $\sigma$ , so it can be identified with  $\mathbf{Z}/s_\chi\mathbf{Z}$ . By definition, the space  $\text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$  has an  $\tilde{l}$ -basis  $(b_i)_{i \in \mathbf{Z}/s_\chi\mathbf{Z}}$  on which the action of  $G_\chi$  is given by

$$\rho(t)(b_i) = \chi(\sigma^i \cdot t)b_i = \chi^{q^i}(t)b_i \quad (t \in T, i \in \mathbf{Z}/s_\chi\mathbf{Z}),$$

and  $\rho(\sigma^{s_\chi})(b_i) = \lambda b_i$ . This action is extended to  $G$  by  $\rho(\sigma)(b_i) = b_{i+1}$  for  $i \not\equiv -1 \pmod{s_\chi}$  and  $\rho(\sigma)(b_{-1}) = \lambda b_0$ , which gives back, as it should, the action of  $\sigma^{s_\chi}$ . Now it is clear that  $\rho_{\bar{\chi}, \lambda}$  depends only on  $(\bar{\chi}, \lambda)$ .

(11) *The  $\tilde{l}$ -representation  $\rho_{\bar{\chi}, \lambda}$  is absolutely irreducible and determines the pair  $(\bar{\chi}, \lambda)$ .* Write  $\rho = \rho_{\bar{\chi}, \lambda}$ . None of the  $T$ -stable lines in  $\rho$  (the  $s_\chi$  lines on which  $T$  acts respectively via the characters  $\chi^{q^i}$ , which are distinct for distinct  $i \in \mathbf{Z}/s_\chi\mathbf{Z}$ ) is stable under  $\sigma$  unless  $s_\chi = 1$ , in which case  $G_\chi = G$  and  $\rho = \chi \otimes \psi_{\chi, \lambda}$ , so  $\rho$  is irreducible in every case, and in fact absolutely irreducible because the same argument works over any finite extension of  $\tilde{l}$ . Note that the  $\Sigma$ -orbit  $\bar{\chi}$  can be recovered from  $\rho$  because  $\rho|_T = \bigoplus_{\eta \in \bar{\chi}} \eta$ , and then  $\lambda \in \tilde{l}^\times$  can be recovered because  $\rho(\sigma^{s_\chi})$  is the homothety of ratio  $\lambda$ .

(12) *Every irreducible  $\bar{\mathbf{F}}_p$ -representations  $\rho$  of  $G$  come from a pair  $(\bar{\chi}, \lambda)$  as in (8).* Here  $\bar{\mathbf{F}}_p$  is a maximal galoisian extension of  $\tilde{l}$ . Let  $\bar{T} = T/\text{Ker}(\rho|_T)$ , so that  $\rho$  comes from an (irreducible)  $\bar{\mathbf{F}}_p$ -representation  $\bar{\rho}$  of  $\bar{G} = \bar{T} \times_q \Sigma$  whose restriction to  $\bar{T}$  is faithful. Let  $P$  be the intersection of the Sylow  $p$ -subgroups of  $\bar{G}$ . The image  $\bar{\rho}(P)$  is trivial because  $P$  is a normal  $p$ -subgroup of  $\bar{G}$ , the characteristic of  $\tilde{l}$  is  $p$ , and  $\bar{\rho}$  is irreducible [11, Chapitre 8, Proposition 26]. So  $\bar{\rho}$  comes from a representation  $\hat{\rho}$  of  $\bar{G}/P$ . Let  $\Sigma'$  denote the kernel of the action of  $\Sigma$  on  $\bar{T}$ , so that the subgroup  $\bar{G}' = \bar{T} \times \Sigma'$  of  $\bar{G}$  is commutative. As  $\bar{G}' \cap P$  is the Sylow  $p$ -subgroup of  $\Sigma'$ ,

the order of  $\hat{\rho}(\bar{G}')$  divides the order of  $\tilde{l}^\times$ , by our definition of  $\tilde{l}$ . It follows that  $\bar{\rho}|_{\bar{G}'}$  is a direct sum of characters  $\bar{G}' \rightarrow \tilde{l}^\times$  such that the restriction to  $\bar{T}$  of at least one of which — call it  $\xi$  — is faithful

(13) View  $\chi = \xi|_{\bar{T}}$  as a character of  $T$ . Since the order  $e$  of  $T$  divides the order  $q^f - 1$  of  $l^\times$ , we have  $\chi(T) \subset l^\times$ . Also,  $\text{Ker}(\chi) = \text{Ker}(\rho|_T)$ , so that  $\bar{G}' = \bar{G}_\chi = T_\chi \times \Sigma_\chi$ , in the previous notation. Recall that  $s_\chi$  is the size of the  $\Sigma$ -orbit  $\bar{\chi}$ , and that  $\Sigma_\chi$  is generated by  $\sigma^{s_\chi}$ . Let  $b_0 \neq 0$  be a vector (in the representation space of  $\rho$ ) on which  $G_\chi$  acts through  $\xi$ , and define  $\lambda \in \tilde{l}^\times$  by  $\xi(\sigma^{s_\chi})(b_0) = \lambda b_0$ . We claim that  $\rho = \rho_{\bar{\chi}, \lambda}$ .

(14) Put  $b_i = \rho(\sigma^i)(b_0)$  for  $i \in [0, s_\chi[$ . Note that  $\rho(\sigma)(b_{s_\chi-1}) = \lambda b_0$  and

$$\rho(t)(b_i) = \rho(t\sigma^i)(b_0) = \rho(\sigma^i t^{q^i})(b_0) = \chi^{q^i}(t)b_i \quad (t \in T, i \in [0, s_\chi[).$$

The characters  $\chi^{q^i}$  are distinct for distinct  $i \in [0, s_\chi[$ , therefore the family  $(b_i)_{i \in [0, s_\chi[}$  is linearly independent. Also, the subspace generated by the  $b_i$  is  $G$ -stable, and in fact equal to  $\rho_{\bar{\chi}, \lambda} = \text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$  as described earlier. Since  $\rho$  is irreducible, we must have  $\rho = \rho_{\bar{\chi}, \lambda}$ , as claimed. Therefore :

(15) *The set of irreducible  $\tilde{l}$ -representations of  $G = T \times_q \Sigma$  is in natural bijection with the set of pairs  $(\bar{\chi}, \lambda)$  consisting of the  $\Sigma$ -orbit  $\bar{\chi}$  of a character  $\chi : T \rightarrow l^\times$  and an element  $\lambda \in \tilde{l}^\times$  of order dividing  $fs_\chi^{-1}$ , where  $s_\chi = \text{Card } \bar{\chi}$ . The pair  $(\bar{\chi}, \lambda)$  gives rise to the induced representation  $\rho_{\bar{\chi}, \lambda} = \text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$ , where  $G_\chi = T \times_q \Sigma_\chi$ ,  $\Sigma_\chi$  is generated by  $\sigma^{s_\chi}$ , and  $\psi_{\chi, \lambda} : \Sigma_\chi \rightarrow \tilde{l}^\times$  is the character such that  $\psi_{\chi, \lambda}(\sigma^{s_\chi}) = \lambda$ . All these representations are absolutely irreducible.*  $\square$

(16) *Some natural characters.* The group  $T$  comes with the faithful character  $\theta : T \rightarrow l^\times$ , so  $G$  has a natural absolutely irreducible  $\tilde{l}$ -representation  $\rho_{\bar{\theta}, 1}$  of degree equal to the order of  $\bar{q} \in (\mathbf{Z}/e\mathbf{Z})^\times$ . We could also consider  $\theta^d$  for various divisors  $d$  of  $e$ . Notice that  $\theta$  allows us to identify  $\text{Hom}(T, l^\times)$  with  $\mathbf{Z}/e\mathbf{Z}$ , and the  $\Sigma$ -orbit of  $\chi = \theta^i$  with the  $\Sigma$ -orbit of  $i \in \mathbf{Z}/e\mathbf{Z}$  (for the action  $\sigma \mapsto (j \mapsto qj)$ ).

(17) Let us now come to irreducible  $\mathbf{F}_p$ -representations  $\pi$  of  $G$ , which are also treated in [7, Proposition 4.2]. The group  $\Phi = \text{Gal}(\tilde{l}|\mathbf{F}_p)$  acts on the set of irreducible  $\tilde{l}$ -representations  $\rho$  of  $G$  by conjugation. Let  $\varphi : x \mapsto x^p$  ( $x \in \tilde{l}$ ) be the canonical generator of  $\Phi$ . If  $\rho$  corresponds to the pair  $(\bar{\chi}, \lambda)$  as above, then  $\varphi\rho$  corresponds to the pair  $(\bar{\chi}^p, \lambda^p)$ . The set of irreducible  $\mathbf{F}_p$ -representations  $\pi$  of  $G$  is in natural bijection with the set of  $\Phi$ -orbits  $R$  for this action ;  $\pi$  and  $R$  correspond to each other if  $\pi \otimes_{\mathbf{F}_p} \tilde{l} = \bigoplus_{\rho \in R} \rho$ . If so, then  $\deg \pi = (\deg \rho)(\text{Card } R)$ , for any  $\rho \in R$ . Regarding this kind of “galoisian descent”, see for example [1, V.60].

(18) Let us compute  $\text{Card } R$ , or the size of the  $\Phi$ -orbit  $\overline{(\bar{\chi}, \lambda)}$  of any pair  $(\bar{\chi}, \lambda)$  such that  $\rho_{\bar{\chi}, \lambda} \in R$ . Recall that  $d_\chi$  is the common order of every  $\chi \in \bar{\chi}$ , and that  $r_\chi$  (resp.  $s_\chi$ ) is the order of  $\bar{p}$  (resp.  $\bar{q}$ ) in  $(\mathbf{Z}/d_\chi \mathbf{Z})^\times$ . (We already know that  $\deg \rho_{\bar{\chi}, \lambda} = s_\chi$ ). The size of the  $\Phi$ -orbit of the  $\Sigma$ -orbit  $\bar{\chi}$  is  $r_\chi s_\chi^{-1}$ , so the number of  $\mathbf{F}_p$ -conjugates of the pair  $(\bar{\chi}, \lambda)$  (or the size of the  $\Phi$ -orbit  $R = \overline{(\bar{\chi}, \lambda)}$ ) is  $\text{lcm}(r_\chi s_\chi^{-1}, w_\lambda)$ , where  $w_\lambda$  is the degree  $[\mathbf{F}_p(\lambda) : \mathbf{F}_p]$  (which obviously depends only on the  $\Phi$ -orbit of  $\lambda$ ), and the degree of  $\pi$  is  $s_\chi \text{lcm}(r_\chi s_\chi^{-1}, w_\lambda) = \text{lcm}(r_\chi, s_\chi w_\lambda)$ . Therefore :

(19) *The set of irreducible  $\mathbf{F}_p$ -representations  $\pi$  of  $G = T \times_q \Sigma$  is in natural bijection with the set of  $\Phi$ -orbits  $R = \overline{(\bar{\chi}, \lambda)}$  of pairs  $(\bar{\chi}, \lambda)$  consisting of the  $\Sigma$ -orbit  $\bar{\chi}$  of a character  $\chi : T \rightarrow l^\times$  and an element  $\lambda \in \tilde{l}^\times$  of order dividing  $f s_\chi^{-1}$ , where  $s_\chi$  is the order of  $\bar{q} \in (\mathbf{Z}/d_\chi \mathbf{Z})^\times$  and  $d_\chi$  is the order of  $\chi$ , under the correspondence  $\pi \otimes_{\mathbf{F}_p} \tilde{l} = \bigoplus_{(\bar{\chi}, \lambda) \in R} \rho_{\bar{\chi}, \lambda}$ , where  $\rho_{\bar{\chi}, \lambda}$  is the absolutely irreducible  $\tilde{l}$ -representation of  $G$  attached to  $(\bar{\chi}, \lambda)$ . If  $r_\chi$  denotes the order of  $\bar{p} \in (\mathbf{Z}/d_\chi \mathbf{Z})^\times$  and  $w_\lambda = [\mathbf{F}_p(\lambda) : \mathbf{F}_p]$ , then  $\deg \pi = \text{lcm}(r_\chi, s_\chi w_\lambda)$ .  $\square$*

(20) *The field of definition.* Let  $k_{\bar{\chi}, \lambda} \subset \tilde{l}$  be the extension of  $\mathbf{F}_p$  of degree  $\text{lcm}(r_\chi s_\chi^{-1}, w_\lambda)$ . It follows for similar reasons that there is a unique (absolutely) irreducible  $k_{\bar{\chi}, \lambda}$ -representation  $\rho'_{\bar{\chi}, \lambda}$  which gives back  $\rho_{\bar{\chi}, \lambda}$  upon changing the base to  $\tilde{l}$  in the sense that  $\rho'_{\bar{\chi}, \lambda} \otimes_{k_{\bar{\chi}, \lambda}} \tilde{l} = \rho_{\bar{\chi}, \lambda}$ ; we call  $k_{\bar{\chi}, \lambda}$  the field of definition of  $\rho_{\bar{\chi}, \lambda}$  and henceforth think of  $\rho_{\bar{\chi}, \lambda}$  as a  $k_{\bar{\chi}, \lambda}$ -representation.

(21) We denote the irreducible  $\mathbf{F}_p$ -representation of  $G$  associated to the  $\Phi$ -orbit  $\overline{(\bar{\chi}, \lambda)}$  by  $\pi_{\overline{(\bar{\chi}, \lambda)}}$ . The degree of  $\pi_{\overline{(\bar{\chi}, \lambda)}}$  is  $r_\theta$  (the order of  $\bar{p} \in (\mathbf{Z}/e \mathbf{Z})^\times$ ). The notation is somewhat ambiguous because it doesn't refer to the group  $G$ . Indeed, if  $l'$  is a finite extension of  $l$ , then the same  $\Phi$ -orbit  $\overline{(\bar{\chi}, \lambda)}$  also gives rise to an irreducible  $\mathbf{F}_p$ -representation  $\pi' = \pi_{\overline{(\bar{\chi}, \lambda)}}$  of the group  $G' = T \times_q \Sigma'$ , where  $\Sigma' = \text{Gal}(l'|k)$ . The saving grace is that if we use the galoisian projection  $\gamma : \Sigma' \rightarrow \Sigma$  to view  $G$  as a quotient of  $G'$ , then  $\pi' = \pi \circ \gamma$ .

(22) We give some examples which will be useful later [5] in classifying quartic extensions  $E$  of a dyadic field  $K$  which have no intermediate quadratic extensions. The set of such  $E$  was parametrised in [4, 14] by the set of pairs  $(\rho, D)$ , where  $\rho$  is an irreducible  $\mathbf{F}_2$ -representation of  $\text{Gal}(\bar{K}|K)$  (and  $\bar{K}$  is the maximal galoisian extension of  $K$ ) and  $D$  is an  $\mathbf{F}_2^2$ -extension of the fixed field  $F_\rho$  of the kernel of  $\rho$  such that  $D$  is galoisian over  $K$  and the resulting conjugation action of  $\text{Gal}(F_\rho|K)$  on  $\text{Gal}(D|F_\rho)$  is given by  $\rho$ . If so, the group  $\text{Gal}(\hat{E}|K)$  (where  $\hat{E}$  is the galoisian closure of  $E$  over  $K$ ) is given by  $\mathbf{F}_2^2 \times_\rho \text{Gal}(F_\rho|K)$  [4]. Here we merely construct all

degree-2 irreducible  $\mathbf{F}_2$ -representations  $\rho$  of certain groups  $G$  and identify the twisted product  $\mathbf{F}_2^2 \times_\rho G$ . Why it suffices to consider only these  $G$  was explained in [4, 15] and will also become clear at the very end.

(23) *A  $(\mathbf{Z}/3\mathbf{Z})$ - and an  $\mathfrak{A}_3$ -example.* Take  $p = 2$ ,  $f = 3$ ,  $e = 1$ , so that  $T = \{1\}$ , and  $G = \Sigma = \mathbf{Z}/3\mathbf{Z}$ . We have  $\tilde{l} = l(\sqrt[3]{1})$ . The only  $\chi : T \rightarrow l^\times$  is the trivial character 1 ; for it, there are three possible  $\lambda$ , namely 1,  $\sqrt[3]{1}$  and  $\sqrt[3]{1}^2$ . So we get three  $\tilde{l}$ -characters, namely  $\rho_{\bar{1},1}$ ,  $\rho_{\bar{1},\sqrt[3]{1}}$  and  $\rho_{\bar{1},\sqrt[3]{1}^2}$  of which the latter two are in the same  $\Phi$ -orbit, and these are the only irreducible  $\tilde{l}$ -representations of  $G$ . Thus we get two  $\mathbf{F}_2$ -representations, namely the trivial representation  $\pi_{\bar{1},1}$  and the irreducible degree-2 representation  $\pi = \pi_{\bar{1},\sqrt[3]{1}}$ ; the latter is not absolutely irreducible. The group  $\mathbf{F}_2^2 \times_\pi G$  is isomorphic to  $\mathfrak{A}_4$ .

Or keep  $p = 2$  and take  $q \equiv 1 \pmod{3}$ ,  $f = 1$ ,  $e = 3$ , so that  $\tilde{l} = l$ . Then  $G = T = \mathfrak{A}_3$  is cyclic of order 3, the three irreducible  $l$ -representations are  $\rho_{\bar{1},1}$ ,  $\rho_{\bar{\theta},1}$ ,  $\rho_{\bar{\theta}^2,1}$  (all three of degree 1) of which the latter two are in the same  $\Phi$ -orbit, so the two irreducible  $\mathbf{F}_2$ -representations are  $\pi_{\bar{1},1}$  (trivial) and  $\pi = \pi_{\bar{\theta},1}$  (degree 2). The group  $\mathbf{F}_2^2 \times_\pi G$  is isomorphic to  $\mathfrak{A}_4$ , as before.

(24) *An  $\mathfrak{S}_3$ -example.* Keep  $p = 2$  and take  $q \equiv -1 \pmod{3}$ ,  $f = 2$ ,  $e = 3$ , so that  $\Sigma = \mathbf{Z}^\times$ ,  $G$  is isomorphic to  $\mathfrak{S}_3$ , and  $\tilde{l} = l$ . The only characters  $T \rightarrow l^\times$  are 1 (of order  $d = 1$ ) and  $\theta, \theta^2$  (of order  $d = 3$ ) ; they fall into two  $\Sigma$ -orbits, namely  $\bar{1}$  (of size  $s = 1$ ) and  $\bar{\theta}$  (of size  $s = 2$ ). The only possible  $\lambda$  in either case is  $\lambda = 1$ . So  $\rho_{\bar{1},1}$  (of degree 1) and  $\rho_{\bar{\theta},1}$  (of degree 2) are the only two (absolutely) irreducible  $l$ -representations of  $G$ , each of which is its own  $\Phi$ -orbit. Therefore there are two irreducible  $\mathbf{F}_2$ -representations of  $G$ , namely  $\pi_{\bar{1},1}$  (the trivial representation) and  $\pi = \pi_{\bar{\theta},1}$  (of degree 2). In fact,  $\pi : G \rightarrow \mathbf{GL}_2(\mathbf{F}_2)$  is an isomorphism, and  $\mathbf{F}_2^2 \times_\pi G$  is isomorphic to  $\mathfrak{S}_4$ .

(25) Another general algebraic observation we need is the following lemma culled from [7, 4.9] ; see also [8, p. 154]. Let  $G$  be any finite group,  $F$  any field,  $E$  a finite galoisian extension of  $F$ ,  $W$  an *absolutely* irreducible  $E$ -representation of  $G$  such that the conjugates  ${}^\sigma W$  ( $\sigma \in \text{Gal}(E|F)$ ) of  $W$  are all inequivalent. By galoisian descent, there is a unique (irreducible)  $F$ -representation  $V$  of  $G$  such that  $V \otimes_F E = \bigoplus_{\sigma \in \text{Gal}(E|F)} {}^\sigma W$ . By Schur's lemma, we have  $\text{End}_{E[G]}(W) = E$  and also  $\text{End}_{F[G]}(V) = E$ .

Let  $m > 0$  be an integer. For every  $a = (a_i)_{i \in [1,m]}$  in  $E^m$ , we have the  $F[G]$ -morphism  $\varphi_a : V \rightarrow V^m$  sending  $x$  to  $(a_i x)_{i \in [1,m]}$  ; it is injective if and only if  $a \neq 0$ . For  $a \neq 0$ , the image  $\varphi_a(V)$  depends only on the line  $\bar{a} \subset E^m$  generated by  $a$ .

(26) The map  $\bar{a} \mapsto \varphi_a(V)$  is a bijection of the set  $\mathbf{P}_{m-1}(E)$  of lines in  $E^m$  with the set of submodules of  $V^m$  isomorphic to  $V$ . In particular, if  $E$  is finite and  $q = \text{Card}(E)$ , then the number of such submodules is  $(q^m - 1)(q - 1)^{-1}$ .

*Proof.* The map in question is injective : indeed, if  $a \neq 0$  and  $b \neq 0$  are in  $E^m$ , and if  $\varphi_a(V) = \varphi_b(V)$ , then (slightly abusing notation)  $\varphi_b^{-1} \circ \varphi_a$  is a  $G$ -automorphism of  $V$ , so a homothety of some ratio  $\xi \in E^\times$ , therefore  $a = \xi b$  and  $\bar{a} = \bar{b}$ . Next, the map  $\bar{a} \mapsto \varphi_a(V)$  is surjective : if  $\psi : V \rightarrow V^m$  is an injective  $G$ -morphism, the maps  $\pi_i \circ \psi$ , where the  $\pi_i : V^m \rightarrow V$  are the canonical projections, are homotheties of some ratio  $a_i \in E$  such that  $a = (a_i)_{i \in [1, m]}$  is  $\neq 0$ , and  $\psi = \varphi_a$ .  $\square$

### 3. Irreducible $\mathbf{F}_p$ -representations over $p$ -fields

(27) Let  $K$  be a  $p$ -field,  $k$  its residue field,  $q = \text{Card } k$ , and let  $V_0$  (resp.  $V$ , resp.  $\tilde{K}$ ) be the maximal unramified (resp. tamely ramified, resp. galoisian) extension of  $K$ . Put  $\Gamma_0 = \text{Gal}(V_0|K)$  and  $\Gamma = \text{Gal}(V|K)$ . We have seen in the Introduction that every irreducible  $\mathbf{F}_p$ -representation of  $\text{Gal}(\tilde{K}|K)$  factors through  $\Gamma$ .

For every  $n > 0$ , put  $e_n = p^n - 1$  and  $V_n = V_0(^e\sqrt[n]{\varpi})$ , where  $\varpi$  is a uniformiser of  $K$ . It doesn't matter which  $\varpi$  we choose because  $V_n$  is also obtained by adjoining the family  $^e\sqrt[n]{x}$  (indexed by  $x \in V_0^\times$ ) to  $V_0$ . Every  $V_n$  is galoisian over  $K$  ; put  $\Gamma_n = \text{Gal}(V_n|K)$ , so that  $V = \varinjlim V_n$  and  $\Gamma = \varprojlim \Gamma_n$ . The salient quotients  $\Gamma_n$  of  $\Gamma$  have nothing to do with the ramification filtration on  $\Gamma$  which is quite simply  $\Gamma^0 \subset \Gamma$ , where  $\Gamma^0 = \text{Gal}(V|V_0)$  is the inertia subgroup. If  $p = 2$ , then  $V_1 = V_0$ . Note that if  $K$  has characteristic 0, then the  $p$ -torsion subgroup  ${}_pV_n^\times$  of  $V_n^\times$  has order  $p$  (because  $V_1$  contains  ${}^{p-1}\sqrt[p]{-p}$ ).

(28) Note that  $V_n$  is the compositum of all finite extensions of  $K$  of ramification index dividing  $e_n$ , so the indexing has something to do with ramification after all. Note also that if  $a = v_p(q)$  is the exponent of  $p$  in  $q$ , then  $V_a$  is the maximal tamely ramified abelian extension of  $K$ .

(29) Let  $n > 0$  be an integer. Every irreducible  $\mathbf{F}_p$ -representation of  $\Gamma$  of degree dividing  $n$  factors through the quotient  $\Gamma_n$  of  $\Gamma$ .

*Proof.* Let  $\pi$  be such a representation, and let  $L$  be a finite unramified extension of the fixed field  $V^{\text{Ker}(\pi)}$  which is split over  $K$  in the sense the inertia subgroup  $G_0$  of  $G = \text{Gal}(L|K)$  has a complement in  $G$  ; by hypothesis,  $\pi|_{G_0}$  is faithful. It suffices (27) to show that the ramification index  $e$  of  $L$  over  $K$  divides  $e_n$ .

Let  $l$  be the residue field of  $L$ . The filtration  $G_0 \subset G$  is split by hypothesis ; the choice of a section  $G/G_0 \rightarrow G$  leads to an isomorphism of  $G$  with  $T \times_q \Sigma$ , where  $\Sigma = \text{Gal}(l|k)$  and  $T \subset l^\times$  is the subgroup of order  $e$ . Since  $\pi|_T$  is faithful,  $\chi|_T$  is faithful for any character  $\chi : T \rightarrow l^\times$  which occurs in  $(\pi|_T) \otimes \tilde{l}$  as in (11). Therefore the order of  $\chi$  is  $e$ . Let  $r$  be the order of  $\bar{p} \in (\mathbf{Z}/e\mathbf{Z})^\times$ , so that  $p^r \equiv 1 \pmod{e}$ . Since  $n$  is a multiple of  $r$  (19), we have  $p^n \equiv 1 \pmod{e}$ , and hence  $e$  divides  $e_n = p^n - 1$ .  $\square$

(30) Since there are only finitely many irreducible  $\mathbf{F}_p$ -representations  $\pi$  of  $\Gamma$  of given degree  $n$  (because  $\Gamma$  is finitely generated and  $\mathbf{GL}_n(\mathbf{F}_p)$  is finite), there are finite extensions  $M$  of  $K$  such that every irreducible  $\mathbf{F}_p$ -representation of  $\Gamma$  of degree  $n$  factors through  $\text{Gal}(M|K)$ . For  $n = 1$ , the smallest possible  $M$  is clearly  $L_1 = K(^{p-1}\sqrt{K^\times})$ , which was used in [2] (and in [6] in the characteristic-0 case) ; recently I've discovered that this observation was made already in [10, V.9].

(31) *A partition.* Notice that *ramified* irreducible  $\mathbf{F}_p$ -representations  $\pi$  of  $\Gamma$  of degree  $n > 0$  can be partitioned into classes labelled by the divisors  $r$  of  $n$ . The representation  $\pi$  belongs to the class labelled by  $r$  if  $r$  is the smallest (in the sense of divisibility) divisor of  $n$  such that  $\pi$  factors through  $\Gamma_r$  ; equivalently,  $r$  is the order of  $\bar{p} \in (\mathbf{Z}/e\mathbf{Z})^\times$ , where  $e$  is the ramification index over  $K$  of the fixed field  $V^{\text{Ker}(\pi)}$ . If  $p = 2$ , then the class of label 1 is  $\emptyset$  because  $\Gamma_1 = \Gamma_0$  and  $\pi$  would be unramified.

(32) For every  $n > 0$ ,  $K_n = K(^{e_n}\sqrt{1})$  is the unramified extension of  $K$  of degree equal to the order  $s_n$  of  $\bar{q} \in (\mathbf{Z}/e_n\mathbf{Z})^\times$  ; put  $L_n = K_n(^{e_n}\sqrt{K_n^\times})$ , so that  $L_n \subset V_n$  and indeed  $V_n = L_n V_0$ . Note that  $L_n$  is the maximal abelian extension of  $K_n$  of exponent dividing  $e_n$ , so it is galoisian over  $K$  ; put  $G_n = \text{Gal}(L_n|K)$ . We have

$$V_0 = \varinjlim K_n, \quad V = \varinjlim L_n, \quad \Gamma = \varprojlim G_n.$$

Note that if  $K$  has characteristic 0, then  $_p L_n^\times$  has order  $p$  (because  $L_1$  contains  $^{p-1}\sqrt{-p}$ ).

In the proof of the next proposition, we shall need to consider certain finite galoisian extensions  $M$  of  $K$ . We denote the residue fields of  $K_n$  (resp.  $L_n$ , resp.  $M$ ) by  $k_n$  (resp.  $l_n$ , resp.  $m$ ). Note that  $L_n$  is split over  $K$  because  $L_n = L_{n,0} (^{e_n}\sqrt{\varpi})$  for any uniformiser  $\varpi$  of  $K$ , where  $L_{n,0}$  is the maximal unramified extension of  $K$  in  $L_n$ . If  $M$  is unramified over  $L_n$ , then  $M$  is also split over  $K$ .

(33) *Every irreducible  $\mathbf{F}_p$ -representation of  $\Gamma$  of degree dividing  $n$  factors through the finite quotient  $G_n = \text{Gal}(L_n|K)$  of  $\Gamma$ .*

*Proof.* Let  $\pi'$  be such a representation, and recall that it factors through  $\Gamma_n$  (28). Let  $M$  be a finite unramified extension of  $L_n$  such



that  $H = \text{Gal}(M|K)$  has the property claimed for  $G_n$  ; we have to show that  $\text{Gal}(M|L_n) \subset \text{Ker}(\pi')$ . Choose a uniformiser  $\varpi$  of  $K$  and identify  $H$  with  $T \times_q \text{Gal}(m|k)$  and  $G_n$  with  $T \times_q \text{Gal}(l_n|k)$  as above ; these identifications are compatible with the galoisian projections  $\gamma : H \rightarrow G_n$  and  $\text{Gal}(m|k) \rightarrow \text{Gal}(l_n|k)$ . The representation  $\pi' = \pi_{\bar{\eta}, \mu}$  of  $H$  in question is associated to the  $\Phi$ -orbit of a pair  $(\bar{\eta}, \mu)$  consisting of the  $\text{Gal}(m|k)$ -orbit of some character  $\eta : T \rightarrow m^\times$  and some  $\mu \in \tilde{m}^\times$  as in (19). We certainly have  $\eta(T) \subset k_n^\times$ , therefore  $\bar{\eta}$  can be viewed as the  $\text{Gal}(l_n|k)$ -orbit  $\bar{\chi}$  of a character  $\chi : T \rightarrow l_n^\times$ . Recall that the degree  $w_\mu = [\mathbf{F}_p(\mu) : \mathbf{F}_p]$  divides  $n$ , therefore the order of  $\mu$  divides  $e_n$ , and hence  $\mu \in k_n^\times$  ; call it  $\lambda$  in this avatar. The  $\Phi$ -orbit of this new pair  $(\bar{\chi}, \lambda)$  gives a representation  $\pi = \pi_{\bar{\chi}, \lambda}$  of  $G_n$ , and  $\pi'$  factors through it ( $\pi' = \pi \circ \gamma$ ), as in (21).  $\square$

(34) *Remark.* We define the *optimal* quotient of  $\Gamma$  in degree  $n$  to be the smallest quotient of  $\Gamma$  through which every irreducible  $\mathbf{F}_p$ -representation  $\pi$  of  $\Gamma$  of degree  $n$  factors. We also say that the corresponding extension  $M_n$  of  $K$  is the *optimal* extension in degree  $n$  ; it is the compositum, over all  $\pi$ , of the extensions  $V^{\text{Ker}(\pi)}$  of  $K$ . For  $n = 1$ , the quotient  $G_1$  of  $\Gamma$  and the corresponding extension  $L_1 = K(\sqrt[p-1]{K^\times})$  of  $K$  are clearly optimal. For  $n > 1$ , the extension  $M_n$  is introduced in [7] but we prefer working with  $L_n$  (which contains  $M_n$  by (33)) because  $L_n$  is very explicit, contains  $\sqrt[p]{1}$  in characteristic 0, and it is split over  $K$  so that the general theory of little groups as explained above can be applied. Note that  $M_n$  contains the unramified extension of  $K$  of degree  $e_n$  and every totally ramified extension of  $K$  of degree dividing  $e_n$ . We haven't checked whether  $M_n = L_n$  in general.

(35) *The  $(\mathbf{Z}/3\mathbf{Z})$ -,  $\mathfrak{A}_3$ - and  $\mathfrak{S}_3$ -examples.* Consider the case  $p = 2$  and  $n = 2$ , so that  $e_2 = 3$ . If  $q \equiv 1 \pmod{3}$ , then we have  $K_2 = K$  and  $L_2 = K(\sqrt[3]{K^\times})$ , so that  $L_2$  contains the unramified cubic extension and the three ramified cubic extensions (all three cyclic) of  $K$ . We thus get back the  $(\mathbf{Z}/3\mathbf{Z})$ - and  $\mathfrak{A}_3$ -examples of (23). If  $q \equiv -1 \pmod{3}$ , then  $[K_2 : K] = 2$ , so that  $L_2$  contains the unramified cubic extension and the unique  $\mathfrak{S}_3$ -extension (namely  $K(\sqrt[3]{1}, \sqrt[3]{\varpi})$ , where  $\varpi$  is a uniformiser) of  $K$ . We thus get back the  $(\mathbf{Z}/3\mathbf{Z})$ -example of (23) and the  $\mathfrak{S}_3$ -example of (24).

## BIBLIOGRAPHY

- [1] BOURBAKI (N). — *Algèbre, Chapitres 4 à 7*, Masson, Paris, 1981, 422 p.
- [2] DALAWAT (C). — *Serre's "formule de masse" in prime degree*, Monatshefte Math. **166** (2012) 1, 73–92. Cf. arXiv:1004.2016v6.

- [3] DALAWAT (C) & LEE (JJ). — *Tame ramification and group cohomology*, J. Ramanujan Math. Soc. **32** (2017) 1, 51–74. Cf. arXiv:1305.2580v4.
- [4] DALAWAT (C). — *Solvable primitive extensions*, arXiv:1608.04673.
- [5] DALAWAT (C). — *Wildly primitive extensions*, arXiv:1608.04183.
- [6] DEL CORSO (I) & DVORNICICH (R). — *The compositum of wild extensions of local fields of prime degree*, Monatsh. Math. **150** (2007) 4, 271–288.
- [7] DEL CORSO (I), DVORNICICH (R) & MONGE (M). — *On wild extensions of a  $p$ -adic field*, J. Number Theory **174** (2017), 322–342. Cf. aXiv:1601.05939.
- [8] DOERK (K) & HAWKES (T). — *Finite soluble groups*, Walter de Gruyter & Co., Berlin, 1992. xiv+891 pp.
- [9] KOCH (H). — *Classification of the primitive representations of the Galois group of local fields*, Invent. Math. **40** (1977) 2, 195–216.
- [10] KOCH (H). — *On the local Langlands conjecture*, Séminaire de théorie des nombres de Grenoble **8** (1979-1980), 1–14.
- [11] SERRE (J-P). — *Représentations linéaires des groupes finis*, Hermann, Paris, 1978, 182 p.